6D

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/469,505	12/22/1999	ROBERT J. STONE	UUN99006	5044

25537 7590 01/27/2005

MCI, INC
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW, 10TH FLOOR
WASHINGTON, DC 20036

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/469,505	**Applicant(s)** STONE ET AL.	
	Examiner Christian La Forgia	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. The amendment filed on 01 July 2004 is noted and made of record.

2. Claims 1-29 have been presented for examination.

Response to Arguments

3. Applicant's arguments filed 01 July 2004 have been fully considered but they are not persuasive.

4. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. In response to applicant's argument that the references fail to show certain features, such as tracking functions, packet is sent to a server providing content and away from central intermediary devices, of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

6. With respect to the Applicant's allegation that neither *Bector* nor *McCanne* teach a tracking router, the Examiner kindly directs the Applicant's attention to MPEP § 2131, in particular the discussion of *ipsissimis verbis. Ipsissimis verbis* states that the elements of the invention must be arranged as required by the claim regardless of the identity of terminology. In other words, the fact that *Bector* and *McCanne* do not use the same terminology as the Applicant,

yet teaches the elements of the claim language, is not enough to distinguish the instant application over the prior art.

7. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., tracking, functions of the tracking router) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). *Bector* shows the use of an intercepting routing device (Figure 1, block 110, column 1, lines 43-64) which the Examiner quotes as being equivalent to the tracking router of the claimed invention. The Examiner would like to point out that where applicant acts as his or her own lexicographer to specifically define a term of a claim, the written description must clearly define the claim term and set forth the definition so as to put one reasonably skilled in the art on notice that the applicant intended to so define that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). In addition, the Applicant fails to meet the requirements of defining a term as set forth in the MPEP § 2106. In order to define a term, the Applicant must do so "with reasonable clarity, deliberateness, and precision" and must " set out his uncommon definition in some manner within the patent disclosure' so as to give one of ordinary skill in the art notice of the change" in meaning. The Applicant fails to clearly, deliberately and precisely claim the function of the tracking router in the claim language. Therefore, the rejection of *Bector* in view of *McCanne* is upheld.

8. See further rejections below.

Claim Rejections - 35 USC § 103

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,687,732 to Bector et al., hereinafter Bector, in view of U.S. Patent No. 6,611,872 to McCanne, hereinafter McCanne.

11. As per claim 1, Bector teaches a method for tracking denial-of-service floods, the method comprising:

rerouting a DoS flood attack datagram to a tracking router (Figure 1 [blocks 107, 110, 114]; column 1, lines 43-64; column 4, lines 9-50; column 14, lines 3-31);

identifying an ingress edge router that forwarded the DoS flood attack datagram (column 4, lines 37-50).

12. Bector teaches identifying the origin computer of the malicious content, thus if the origin computer can be identified the ingress edge router that received the malicious datagram can be identified.

13. Bector does not disclose wherein the tracking router forms an overlay tracking network with respect to an egress edge router.

14. McCanne discloses that is known to use an overlay tracking network to track data over an intended path. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the proxy server form an overlay tracking network as taught by McCanne, since McCanne states at column 2, lines 40-66 that such a modification would allow the system to manage the denial of service attack more intelligent, bandwidth-efficient manner.

15. Regarding claim 2, Bector teaches further comprises executing security diagnostic functions (column 4, lines 9-50).

16. With regards to claims 3 and 15, Bector teaches wherein the security diagnostic functions comprise input debugging (column 4, lines 9-50).

17. Regarding claims 4 and 16, McCanne teaches wherein the overlay tracking network is within an autonomous system that is different from another autonomous system corresponding to the ingress edge router and the egress edge router (Figures 1, 2; column 6, line 65 to column 7, line 40).

18. With regards to claims 5, 11, and 17, McCanne teaches further comprising providing routing information by the overlay tracking network to the ingress edge router and the egress edge router using an inter-administrative-domain routing/signaling protocol (column 4, lines 52-66; column 17, lines 9-60).

19. Concerning claims 6, 12, and 18, McCanne teaches wherein the inter-administrative-domain routing/signaling protocol is BGP (Border Gateway Protocol) (column 4, lines 52-66; column 17, lines 9-60).

20. Regarding claims 7, 19, and 23, McCanne teaches further comprising communicating between the edge routers and the tracking router via tunnels that are created over an unreliable datagram delivery service protocol (column 4, lines 53-65; column 6, lines 11-26).

21. Regarding claims 8, 20, and 24, McCanne teaches further comprising communicating between the edge routers and the tracking router via virtual connections over a separate lower layer protocol (column 6, line 65 to column 7, line 32).

22. Regarding claims 9, 21 and 25, McCanne teaches further comprising communicating between the edge routers and the tracking router via physical connections (Figure 1 [access link]; column 7, lines 32-40).

23. Regarding claim 10, Bector teaches further comprising routing the DoS flood attack datagram from the ingress edge router to the tracking router, wherein the egress edge router has a static route to the victim (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31).

24. Concerning claims 13 and 27, Bector teaches further comprising establishing another static route between the egress router and an external router associated with a victim node, the victim node receiving the DoS flood attack datagram (column 8, line 50 to column 9, line 30).

25. As per claim 14, McCanne teaches a communication system for tracking denial-of-service (DoS) floods, the communication system comprising:

a plurality of edge routers including an ingress edge router and an egress edge router, (Figures 1, 2, 4a, 4b, 4c, 5; column 5, lines 29-63; column 16, line 66 to column 17, line 43);

a tracking router adjacent to the egress edge router, the tracking router being configured to perform the security diagnostic functions, (Figures 1, 2, 4a, 4b, 4c, 5; column 5, lines 29-63; column 16, line 66 to column 17, line 43).

26. McCanne does not disclose each of the edge routers being configured to perform security diagnostic functions, in part, to identify a DoS flood attack datagram, wherein the ingress edge router is associated with a source of the DoS flood attack datagram and the ingress edge router rerouting the DoS flood attack datagram to the tracking router as to permit identification of the ingress edge router, wherein the tracking router forms an overlay tracking network with respect to the plurality of edge routers.

27. Bector discloses that is its known for routers to perform security diagnostics, which include identifying a DOS attack, and rerouting the malicious datagram to an overlay network. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the security diagnostic functions as taught by Bector, since Bector states at column 4, lines 2-54 that such a modification would increase network security.

28. Regarding claim 22, McCanne teaches wherein the overlay tracking network further comprises additional tracking routers (column 7, lines 32-40).

29. Regarding claim 26, Bector teaches wherein the ingress edge router routes the DoS flood attack datagram to the tracking router due to a dynamic routing update from the tracking router (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31).

30. Claims 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bector.

31. As per claim 28, Bector teaches a computer-readable medium carrying one or more sequences of one or more instructions for tracking denial-of-service floods (DoS), the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving a DoS flood attack datagram (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31);

identifying the DoS flood attack datagram (Figure 1 [blocks 107, 114]; column 4, lines 9-50; column 14, lines 3-31);

identifying a previous hop router associated with the DoS flood attack datagram to ultimately locate an ingress adjacency and an ingress adjacency associated with the DoS flood attack (column 4, lines 37-50). Bector does not teach identifying previous hops. Bector teaches identifying the origin computer of the malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made to locate the previous hops, since it has been held that Bector identifies the origin of the malicious datagrams.

32. Regarding claim 29, Bector teaches wherein the computer readable medium further includes instructions for causing the one or more processors to perform the steps of:

instructing the previous hop router to identify a respective previous hop router associated with the DoS flood attack datagram (column 4, lines 37-50). Bector does not teach identifying previous hops. Bector teaches identifying the origin computer of the malicious content. It would have been obvious to one of ordinary skill in the art at the time the invention was made to locate the previous hops, since it has been held that Bector identifies the origin of the malicious datagrams.

Conclusion

33. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

34. The following patents are cited to further show the state of the art with respect to tracking attacks over a network, such as:

United States Patent No. 6,687,833 to Osborne et al., which is cited to show passive network security system capable of diverting and tracking potential attacks for use in a system implementing a network protocol stack.

United States Patent No. 6,654,882 to Froutan et al., which is cited to show a network intrusion detection system designed to stop attackers from gaining unauthorized access.

United States Patent No. 6,442,694 to Bergman et al., which is cited to show tracking of malicious content through a network by transmitting messages betweens nodes indicating that the sending node detected an attack at the message transmitting node.

35. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

36. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

37. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

38. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

39. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
Clf

Gregory J. Lamarre
Primary Examiner